IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

K.MIZRA LLC v. CA, INC.	)	CASE NO. 2:21-cv-00247-JRG (Lead Case)
K.MIZRA LLC v. FORESCOUT TECHNOLOGIES INC.	)	CASE NO. 2:21-cv-00248-JRG (Member Case)
K.MIZRA LLC **v.** **FORTINET, INC.**	)	**CASE NO. 2:21-cv-00249-JRG** **(Member Case)**

DEFENDANT FORTINET, INC.'S ANSWER AND DEFENSES TO THE FIRST AMENDED COMPLAINT OF PLAINTIFF K.MIZRA LLC

As and for its Answer and Affirmative Defenses in response to Plaintiff K.Mizra LLC's ("K.Mizra" or "Plaintiff") First Amended Complaint (Dkt. No. 41), Defendant Fortinet, Inc. ("Fortinet"), by and through its attorneys, states as follows:

NATURE OF THE CASE

1. This is an action for the infringement of U.S. Patent Nos. 8,234,705 (the "'705 patent"), 9,516,048 ("the '048 patent"), and 8,965,892 (the "'892 patent") or also referred to as "the Patents-in-Suit."

ANSWER: Fortinet admits that the pleading purports to be an action of infringement of U.S. Patent Nos. 8,234,705 (the "'705 patent"), 9,516,048 ("the '048 patent"), and 8,965,892 (the "'892 patent") or also referred to as "the Patents-in-Suit." Fortinet denies that the First Amended Complaint properly states a claim or claims, and specifically denies any wrongdoing.

2. Defendant Fortinet has been making, selling, using and offering for sale computer network security products and related services such as FortiNAC, the FortiNAC Server, FortiNAC Control Server, and FortiNAC Application Server, the Endpoint compliance feature set, FortiNAC Agents, FortiNAC Polices (including at least the Endpoint Compliance Policies and Endpoint Compliance Configurations), Admin Scan Configurations (including the Remediation Configuration), Scans, including with the Scan on Connect option, Custom Scans, and various other Fortinet network equipment, including the FortiNAC appliances (e.g., the FortiNAC-CA-500C, 500C 600C, 700C, and FortiNAC-M-500C), and software and related services, including the FortiNAC Virtual Machine, incorporating similar technology that infringes the '705 and '048 patents in violation of 35 U.S.C. § 271 (collectively, "the '705/'048 Accused Instrumentalities").

ANSWER: Fortinet admits it has made, sold, and offered for sale computer network security products. Fortinet denies the remaining allegations of paragraph 2.

3. Defendant Fortinet has been making, selling, using and offering for sale computer email security products such as FortiMail, including the Session Profile, the Sender Reputation feature, FortiGuard's IP Reputation feature, and various other Fortinet network equipment, Fortinet Appliances (including, the FORTIMAIL 200F, 400F, and 900F) and software, including Virtual Machines, incorporating similar technology that infringe the '892 patent in violation of 35 U.S.C. § 271 (collectively, "the '892 Accused Instrumentalities").

ANSWER: Fortinet admits it has been made, sold, and offered for sale computer email security products. Fortinet denies the remaining allegations of paragraph 3.

4. Plaintiff K.Mizra seeks appropriate damages and prejudgment and post-judgment interest for Fortinet's infringement of the Patents-in-Suit.

ANSWER: Fortinet admits that Plaintiff seeks "appropriate" damages and prejudgment and post-judgment interest, but Fortinet denies that it has infringed any of the patents asserted in the First Amended Complaint and further denies that Plaintiff is entitled to any relief.

THE PARTIES

5. Plaintiff K.Mizra is a Delaware limited liability company with its principal place of business at 777 Brickell Ave, #500-96031, Miami, FL 33131. K.Mizra is the assignee and owner of the Patents-in-Suit.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 5, and therefore denies the same.

6. K.Mizra recently relocated its office from California to Florida in the summer of 2021.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 6, and therefore denies the same.

7. Defendant Fortinet is a corporation organized under the laws of Delaware, with a place of business located at 6111 W. Plano Parkway, Plano, TX 75093. Fortinet is registered to conduct business in the state of Texas and has appointed Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process.

ANSWER: Fortinet admits that it is a Delaware corporation, has a principal office in Sunnyvale, CA, and has a location in Plano, Texas. Fortinet admits it is a registered to do business in the state of Texas and has appointed Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, located at 211 E. 7th St., Suite 620, Austin, TX 78701 as its registered for service of process.

8. By maintaining facilities in Plano, Fortinet has a regular and established place of business in the Eastern District of Texas.

ANSWER: Fortinet admits that is has a location in Plano, Texas. Fortinet otherwise denies the remaining allegations in paragraph 8.

9. K.Mizra sent letters to Fortinet in January 2021 and then again in February 2021 about taking a license to K.Mizra's patent portfolio. Prior to K.Mizra filing this lawsuit with its Original Complaint, Fortinet did not respond to any of K.Mizra's correspondence regarding taking a license to K.Mizra's patents..

ANSWER: Fortinet admits that it received letters from K.Mizra. Fortinet otherwise denies the remaining allegations in paragraph 9.

10. Fortinet has been on notice of its infringement of the Patents-in-Suit at least as of the date of service of the Original Complaint on July 8, 2021.

ANSWER: Paragraph 10 states legal conclusions to which no response is required. To the extent that a response is required, Fortinet denies the allegations of paragraph 10.

11. Notwithstanding its receipt of notice that the '705/'048 Accused Instrumentalities and the '892 Accused Instrumentalities infringe the Patents-in-Suit, including notice provided as of the service of the Original Complaint on July 8, 2021, Fortinet continues to sell these Accused Instrumentalities in flagrant disregard of K.Mizra's rights under the Patents-in-Suit.

ANSWER: Paragraph 11 states legal conclusions to which no response is required. To the extent that a response is required, Fortinet denies the allegations of paragraph 11.

JURISDICTION AND VENUE

12. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

ANSWER: Fortinet admits that Plaintiff has brought suit under the patent laws of the United States, Title 35 of the United States Code, but Fortinet denies that it has infringed any of the patents asserted in the First Amended Complaint and further denies that Plaintiff is entitled to any relief.

13. This Court has original subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

ANSWER: Fortinet admits that this pleading appears to be an action for patent infringement under the Patent Laws of the United States, Title 35 of the United States Code. Fortinet denies that the First Amended Complaint properly states such claims, and specifically denies any wrongdoing or infringement. Fortinet admits that the First Amended Complaint purports to base subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a). The remainder of this paragraph contains legal conclusions to which no answer is required.

14. This Court has personal jurisdiction over Fortinet because, *inter alia*, Fortinet has a continuous presence in, and systematic contact with, this District and has registered to conduct business in the state of Texas.

ANSWER: For purposes of this case only, Fortinet does not deny that it is subject to personal jurisdiction in this District. Fortinet otherwise denies the allegations in paragraph 14.

15. Fortinet has committed and continues to commit acts of infringement of K.Mizra's Patents-in-Suit in violation of the United States Patent Laws, and has made, used, sold, offered for

sale, marketed and/or imported infringing products into this District. Fortinet's infringement has caused substantial injury to K.Mizra, including within this District.

ANSWER: Fortinet denies the allegations of paragraph 15.

16. Venue is proper in this District pursuant to 28 U.S.C. §§ 1400 and 1391 because Fortinet has committed acts of infringement in this District and maintains a regular and established place of business in this District.

ANSWER: Paragraph 16 states legal conclusions to which no response is required. To the extent that a response is required, Fortinet denies the allegations of paragraph 16.

THE PATENTS-IN-SUIT

A. U.S. Patent 8,234,705 and U.S. 9,516,048

17. The '705 patent is titled "Contagion Isolation and Inoculation" and was issued by the United States Patent Office to inventors James A. Roskind and Aaron R. Emigh on July 31, 2012. The earliest application related to the '705 patent was filed on September 27, 2004. A true and correct copy of the '705 patent is attached as Exhibit A.

ANSWER: Fortinet admits that U.S. Patent No. 8,234,705 ("the '705 patent") appears to be titled "Contagion Isolation and Inoculation," James A. Roskind and Aaron R. Emigh appear to be the inventors listed on the '705 patent, and the '705 patent appears to have issued on July 31, 2012, and purports to claim priority to U.S. Provisional Patent Application No. 60/613,909 filed on September 27, 2004. Fortinet admits that Exhibit A to the First Amended Complaint purports to be the '705 patent. Fortinet is without to form a belief of the truth or falsity of the remaining allegations of paragraph 17, and therefore denies the same.

18. K.Mizra is the owner of all right, title and interest in and to the '705 patent with the full and exclusive right to bring suit to enforce the '705 patent.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the remaining allegations of paragraph 18, and therefore denies the same.

19. The '705 patent is valid and enforceable under the United States Patent Laws.

ANSWER: Paragraph 19 states legal conclusions to which no response is required. To the extent that a response is required, Fortinet denies the allegations of paragraph 19.

20. The '048 patent is titled "Contagion Isolation and Inoculation Via Quarantine" and was issued by the United States Patent Office to inventors Aaron R. Emigh and James A. Roskind on December 6, 2016. The earliest application related to the '048 patent was filed on September 27, 2004. A true and correct copy of the '048 patent is attached as Exhibit B.

ANSWER: Fortinet admits that U.S. Patent No. 9,516,048 ("the '048 patent") appears to be titled "Contagion Isolation and Inoculation Via Quarantine," Aaron R. Emigh and James A. Roskind appear to be the inventors listed on the '048 patent, and the '048 patent appears to have issued on December 6, 2016, and purports to claim priority to U.S. Provisional Patent Application No. 60/613,909 filed on September 27, 2004. Fortinet admits that Exhibit B to the First Amended Complaint purports to be the '048 patent. Fortinet is without to form a belief of the truth or falsity of the remaining allegations of paragraph 20, and therefore denies the same.

21. K.Mizra is the owner of all right, title and interest in and to the '048 patent with the full and exclusive right to bring suit to enforce the '048 patent.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the remaining allegations of paragraph 21, and therefore denies the same.

22. The '048 patent is valid and enforceable under the United States Patent Laws.

ANSWER: Paragraph 22 states legal conclusions to which no response is required. To the extent that a response is required, Fortinet denies the allegations of paragraph 22.

23. The claims of the '705 and '048 patents are directed to technological solutions that address specific challenges grounded in computer network security. The security of computer systems and networks is a tremendous concern for modern enterprises, since a breach of an internal network can have severe repercussions, including major financial losses, data theft, disclosure of sensitive information, network disruptions, and data corruption—any of which could have devastating consequences to a business, at any scale. The inventors of the '705 and '048 patents understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions into the network, the most exploitable vulnerabilities of a computer network are the end-user computers that roam throughout various other public and private network domains and then access the presumably secure network day in and day out.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 23, and therefore denies the same.

24. For example, the '705 patent explains that "[l]aptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization; and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person." *See, e.g.*, Exhibit A at 1:14-31.

ANSWER: Fortinet admits that paragraph 24 appears to quote 1:14-31 from the '705 patent. Fortinet is without information sufficient to form a belief of the truth or falsity of the remaining allegations of paragraph 24, and therefore denies the same.

25. While Information Technology (IT) engineers may have been able to keep on-site systems secure and up to date with the technology available at that time, they still faced challenges with off-site devices such as a worker's personal laptop or mobile device which posed significant security risks that could allow attackers or viruses stealth access into a business's network, bypassing IT security measures. For example, the '705 patent states that "[u]pon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm." *See, e.g.*, Exhibit A at 1:34-38.

ANSWER: Fortinet admits that paragraph 25 appears to quote 1:34-38 from the '705 patent. Fortinet is without information sufficient to form a belief of the truth or falsity of the remaining allegations of paragraph 25, and therefore denies the same.

26. The invention of the '705 and '048 patents close this loophole by verifying that any device attempting to access a company's network meets the company's standards for network security and will not introduce dangerous computer programs or viruses into the company's network. For example, the '705 patent describes that when "a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is required to be quarantined. According to the '705 and '048 patents, if the host is required to be quarantined, the host is provided only limited access to the protected network. *See, e.g.*, Exhibit A at 3:13-20, Exhibit B at 11:58-66. In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to

be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed." *See* Exhibit A at 3:8-20, Exhibit B at 12:21-28. The '705 and '048 patents further describe that "attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user." Exhibit A at 3:20-23, Exhibit B at 12:28-33.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 26, and therefore denies the same.

27. The '705 and '048 patents disclose an improvement in computer functionality related to computer network security. For instance, an infected host computer with malicious code, such as a computer virus, worm, exploits and the like ("malware"), poses a serious threat if the malware spreads to other hosts in a protected network. Exhibit A at 1:14-41, Exhibit B at 1:42-46. The claims of the '705 and '048 patents employ techniques, unknown at the time of the invention, that do more than detect malware *per se*. The claimed techniques quarantine an infected host to prevent it from spreading malware to other hosts while still permitting limited communications with the network to remedy the malware. As a result, the '705 and '048 patents provide a technological solution to a problem rooted in computer technology by improving the way networks are secured. Through the implementation and provision of this technology by network security companies such as Fortinet, businesses are able to increase their security from vulnerable elements that access their networks.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 27, and therefore denies the same.

28. The claims of the '705 and '048 patents address the technological problems not by a mere nominal application of a generic computer to practice the invention, but by carrying out particular improvements to computerized network security technology in order to overcome problems specifically grounded in the field of computer network security. As the '705 and '048 patents explain, determining whether a quarantine is required involves detection by a computing device, router, firewall, or other network component as to the infestation or cleanliness of a computer. Exhibit A at 11:15-28, Exhibit B at 11:35-49. Moreover, the subsequent steps such as quarantining, limiting network access, remediation, and redirecting network communications are functions fundamentally rooted in computer network technology.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 28, and therefore denies the same.

29. The claims of the '705 and '048 patents recite subject matter that is not merely the routine or conventional use of computer network security that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of assessing and responding to an external network access request in a way that protects the computer network and systems from malicious or undesired breaches. The claims of the '705 and '048 patents specify how a secure

network can assess and respond to an external network access request without jeopardizing network integrity.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 29, and therefore denies the same.

B. U.S. Patent 8,965,892

30. The ’892 patent is titled “Identity-Based Filtering” and was issued by the United States Patent Office to inventor Aaron T. Emigh on February 24, 2015. The earliest application related to the ’892 patent was filed on January 4, 2007. A true and correct copy of the ’892 patent is attached as Exhibit C.

ANSWER: Fortinet admits that U.S. Patent No. 8,965,892 (“the ’892 patent”) appears to be titled “Identity-Based Filtering,” Aaron T. Emigh appears to be the inventors listed on the ’892 patent, and the ’892 patent appears to have issued on February 24, 2015, and purports to claim priority to U.S. Provisional Patent Application No. 60/878,761 filed on January 4, 2007. Fortinet admits that Exhibit C to the First Amended Complaint purports to be the ’892 patent. Fortinet is without to form a belief of the truth or falsity of the remaining allegations of paragraph 30, and therefore denies the same.

31. K.Mizra is the owner of all right, title and interest in and to the ’892 patent with the full and exclusive right to bring suit to enforce the ’892 patent.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 31, and therefore denies the same.

32. The ’892 patent is valid and enforceable under the United States Patent Laws.

ANSWER: Paragraph 32 states legal conclusions to which no response is required. To the extent that a response is required, Fortinet denies the allegations of paragraph 32.

33. The claims of the ’892 patent are directed to technological solutions that address specific challenges rooted in computing technology involving the filtering of electronic content. With the proliferation of electronic documents and content on the internet such as PDFs, webpages, and electronic mail that are accessible via a network address or that traverse a computer network, there is a myriad of undesirable content that a computer user may encounter. *See* Exhibit C at 1:19-22. The inventors of the ’892 patent understood the shortcomings of the traditional

approaches to filtering unwanted content that were solely based on including or excluding certain addresses or uniform resource locators (URLs) associated with the document. The '892 patent explains that prior to its invention, "[a] variety of approaches to content filtering have been employed to avoid undesirable content. Examples of such approaches include blacklisting and whitelisting URLs and sites. However, these approaches fail to discriminate between specific content owners or creators within a site. In some cases, particular participants in a site or service may have more desirable, or less desirable, content than other participants, and present approaches are unable to take advantage of this, leading to either inclusion of objectionable content, or exclusion of desirable content." *Id*. at 1:23-32.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 33, and therefore denies the same.

34. The technological invention of the '892 patent improves upon these conventional techniques for computerized filtering of electronic documents over the internet by extracting and resolving certain data inherent in the electronic document to correlate and determine the reputations of the author or sender of the document and the group in which he or she may be a member of. For example, the '892 patent describes "extracting an identity from a document and/or metadata" and analyzing content with "content analyzing technologies" such as Bayesian filtering or Support Vector Machines. *See, e.g., id.* at 2:24-36. The '892 patent also discusses further steps of correlating identity, detecting affiliation, and determining reputation associated with electronic documents over a computer network. *Id*. at 1:38-63. The enhanced filtration techniques taught by the '892 patent can be carried out "programmatically via an API or by retrieving one or more pages from the network and analyzing them." *See, e.g., id.* at 6:5-67.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 34, and therefore denies the same.

35. The '892 patent claims a way to solve technological problems that existed within the field of electronic documents and computer technology. It provides a technological solution to a problem specific to technology related to electronic documents by improving computer functionality for filtering electronic documents. Faced with the shortcomings of plain filtering techniques such as white-listing or black-listing that existed at the time of the invention, the inventors of the '892 patent developed a far more advanced approach with specific steps for determining and correlating group-related reputation and identity reputation. By utilizing such improvements to electronic content filtering technology, data security companies such as Cisco are able to take advantage of more optimally tailored filtering to block unwanted documents such as electronic mail on computer networks without sacrificing the over-exclusion of desired content.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 35, and therefore denies the same.

36. The way in which the claims of the '892 patent address the technological problem is not merely a nominal application of a generic computer to practice the invention. Instead, the

claims of the '892 patent implement particular improvements to computerized data filtering technology in order to overcome the problems specifically arising in the field of electronic content filtering.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 36, and therefore denies the same.

37. The claims of the '892 patent recite subject matter that is not merely the routine or conventional use of filtering undesired electronic documents that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of determining the reputation associated with electronic documents. The '892 patent claims specify improved computer functionality for extracting certain information and data inherent in the electronic documents for purposes of resolving the reputations associated with the document, author of the document, and groups of which the author may be a member.

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 37, and therefore denies the same.

FIRST CAUSE OF ACTION
(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of '705 PATENT)

38. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

ANSWER: Fortinet repeats and re-alleges its responses to the preceding paragraphs of the First Amended Complaint as if those responses have been fully set forth herein.

39. On information and belief, Fortinet has directly and indirectly infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 19, of the '705 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to the '705/'048 Accused Instrumentalities.

ANSWER: Fortinet denies the allegations of paragraph 39.

40. For example, Claim 19 of the '705 patent recites the following:

> [preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes:

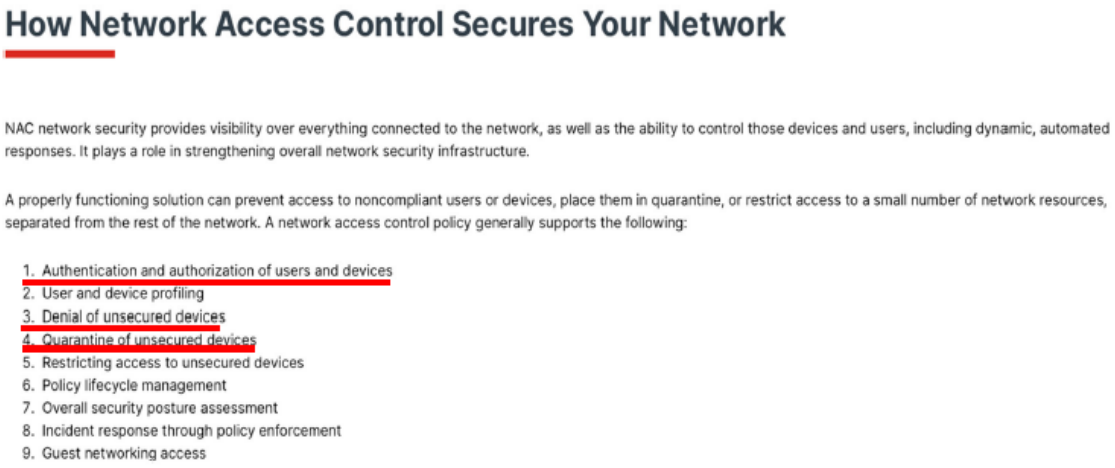
> [B1] contacting a trusted computing base associated with a trusted platform module within the first host,
>
> [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,
>
> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,
> >
> > [E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and
>
> [F] permitting the first host to communicate with the remediation host.

ANSWER: Fortinet admits that paragraph 40 appears to recite claim 19 of the '705 patent.

41. On information and belief, and based on publicly available information, at least the '705/'048 Accused Instrumentalities satisfy each and every limitation of at least claim 19 of the '705 patent.

ANSWER: Fortinet denies the allegations of paragraph 41.

42. The preamble recites a "computer program product for protecting a network." To the extent the preamble is determined to be limiting, the '705/'048 Accused Instrumentalities provide the features described in the preamble. For example, Fortinet describes NAC (Network Access Control) as at least including, authentication and authorization of devices, denial of unsecured devices, and quarantine of unsecured devices:



How Network Access Control Secures Your Network

NAC network security provides visibility over everything connected to the network, as well as the ability to control those devices and users, including dynamic, automated responses. It plays a role in strengthening overall network security infrastructure.

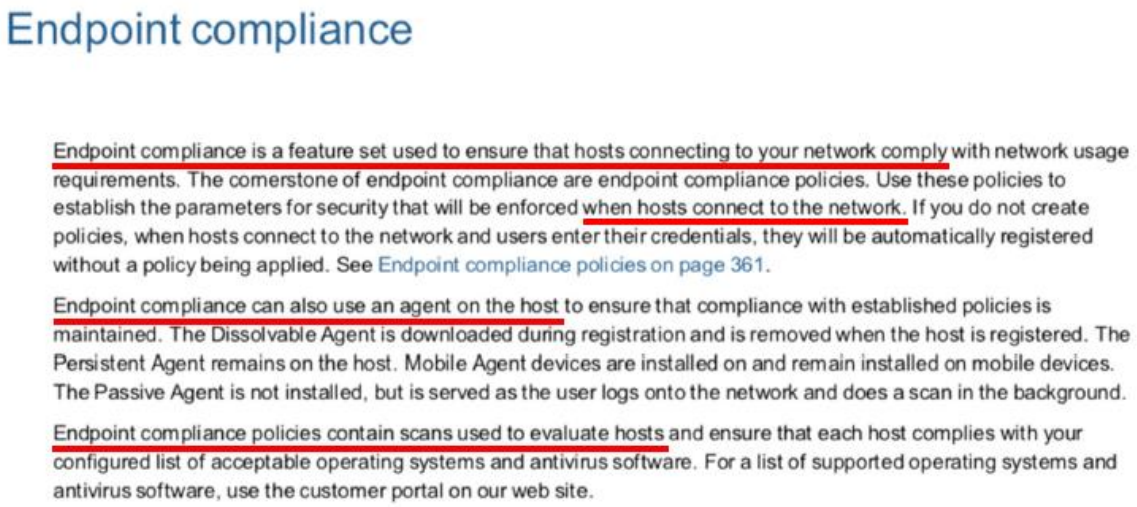
A properly functioning solution can prevent access to noncompliant users or devices, place them in quarantine, or restrict access to a small number of network resources, separated from the rest of the network. A network access control policy generally supports the following:

1. Authentication and authorization of users and devices
2. User and device profiling
3. Denial of unsecured devices
4. Quarantine of unsecured devices
5. Restricting access to unsecured devices
6. Policy lifecycle management
7. Overall security posture assessment
8. Incident response through policy enforcement
9. Guest networking access

See Exhibit E, Network Access Control (NAC) at "How Network Access Control Secures Your Network" (underlining added). To implement NAC, the FortiNAC product line includes hardware appliances (including the FortiNAC-CA-500C, 500C 600C, 700C, and FortiNAC-M-500C), virtual machines, and licenses, where each FortiNAC deployment requires both a Control and Application server. *See id* at "Models and Specifications." The FortiNAC user interface is browser based and is hosted by the FortiNAC appliance. *See* Exhibit D, FortiNAC Administration Guide at 4, "Login procedure."

ANSWER: Fortinet admits part of the preamble of claim 19 of the '705 patent recites a "computer program product for protecting a network." Fortinet denies the remaining allegations of paragraph 42.

43. FortiNAC further provides the "endpoint compliance" feature set that ensures hosts connecting to the network comply with usage requirements, by utilizing host-side agents that scan and evaluate hosts:



Endpoint compliance

Endpoint compliance is a feature set used to ensure that hosts connecting to your network comply with network usage requirements. The cornerstone of endpoint compliance are endpoint compliance policies. Use these policies to establish the parameters for security that will be enforced when hosts connect to the network. If you do not create policies, when hosts connect to the network and users enter their credentials, they will be automatically registered without a policy being applied. See Endpoint compliance policies on page 361.

Endpoint compliance can also use an agent on the host to ensure that compliance with established policies is maintained. The Dissolvable Agent is downloaded during registration and is removed when the host is registered. The Persistent Agent remains on the host. Mobile Agent devices are installed on and remain installed on mobile devices. The Passive Agent is not installed, but is served as the user logs onto the network and does a scan in the background.

Endpoint compliance policies contain scans used to evaluate hosts and ensure that each host complies with your configured list of acceptable operating systems and antivirus software. For a list of supported operating systems and antivirus software, use the customer portal on our web site.

See, e.g., Exhibit D, FortiNAC Administration Guide at 434 (underlining added). Additionally, FortiNAC agents are used to scan hosts and determine whether the host complies with the endpoint compliance policy assigned to that host. *See id.* at 438.

ANSWER: Fortinet denies the allegations of paragraph 43.

44. Thus, to the extent the preamble of claim 19 is limiting, the '705/'048 Accused Instrumentalities meet it.

ANSWER: Fortinet denies the allegations of paragraph 44.

45. Limitation A requires "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation A of claim 19. For example, the FortiNAC "Scans view" allows administrators to configure host scans for compliance, including when a host connects to the network. *See id.* at 384. Additionally, administrators can configure scans to "Scan on Connect," which forces a rescan every time the assigned host connects to the network:

Settings

Field	Definition
Scan Name	Each scan must have a unique name.
Remediation	Indicates when the host is moved to Remediation. Options include: **On Failure**: Host is moved to remediation immediately after failing a scan. **Delayed**: Host is moved to remediation after a user specified delay if the reason for the scan failure has not been addressed. **Audit Only**: Host is scanned and a failure report is generated, but the host is never moved to remediation.
Scan On Connect	Indicates whether this option is enabled or disabled. Scan On Connect forces a rescan every time the host assigned this scan connects to the network. See Scan on connect on page 386. This option only affects hosts running the Persistent Agent.

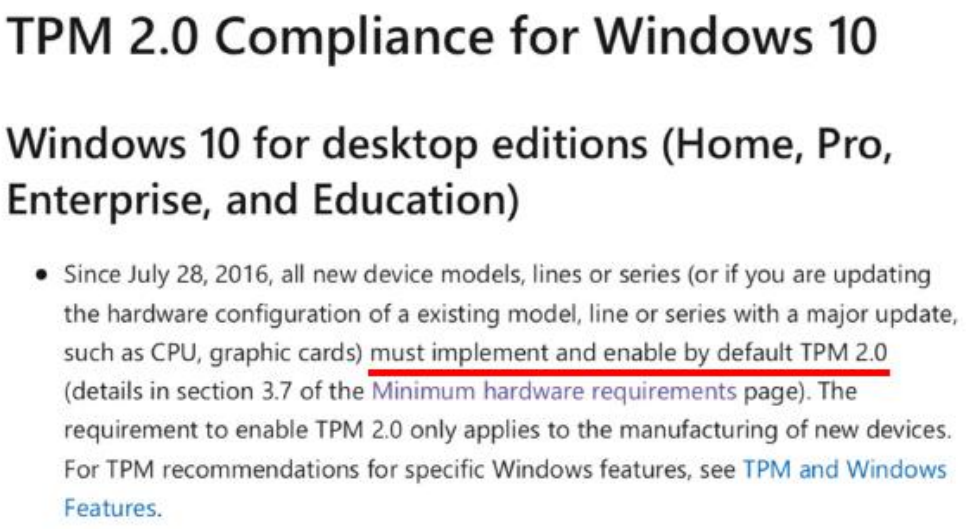
See id. (underlining added). Therefore, the '705/'048 Accused Instrumentalities meet limitation A of claim 19.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." Fortinet denies the remaining allegations of paragraph 45.

46. Limitation B1 requires that "detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation B1 of claim 19. For example, FortiNAC provides several types of agents. FortiNAC agents are used to scan hosts and determine whether the host complies with the endpoint compliance policy assigned to that host. *See id.* at 438. The FortiNAC agent uses a secure encrypted connection to communicate with the FortiNAC Server. Secure connections utilize cryptographically secure random numbers. The FortiNAC agent invokes APIs that generate cryptographically secure random numbers that are seeded in part by the trusted platform module ("TPM"). By making this connecting code that invokes these APIs, Fortinet makes the Accused Instrumentalities that are associated with a TPM.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." Fortinet denies the remaining allegations of paragraph 46.

47. Further, as of July 28, 2016, Windows 10 requires all new devices to implement and enable by default TPM 2.0:



TPM 2.0 Compliance for Windows 10

Windows 10 for desktop editions (Home, Pro, Enterprise, and Education)

- Since July 28, 2016, all new device models, lines or series (or if you are updating the hardware configuration of a existing model, line or series with a major update, such as CPU, graphic cards) must implement and enable by default TPM 2.0 (details in section 3.7 of the Minimum hardware requirements page). The requirement to enable TPM 2.0 only applies to the manufacturing of new devices. For TPM recommendations for specific Windows features, see TPM and Windows Features.

See Exhibit H, "TPM Recommendations" at "TPM 2.0 Compliance for Windows 10" (available at https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations, last visited June 29, 2021) (underlining added).

ANSWER: Fortinet is without information sufficient to form a belief of the truth or falsity of the allegations of paragraph 47, and therefore denies the same.

48. Therefore, the '705/'048 Accused Instrumentalities meet limitation B1 of claim 19.

ANSWER: Fortinet denies the allegations of paragraph 48.

49. Limitation B2 requires that "detecting the insecure condition includes" "receiving a response and determining whether the response includes a valid digitally signed attestation of cleanliness." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation B2 of claim 19. For example, FortiNAC provides several types of agents. *See* Exhibit D, FortiNAC Administration Guide at 438. Moreover, once installed, the Persistent Agent remains installed on the host at all times, running in the background and communicating with FortiNAC. *See id.* at 439. Moreover, SSL certificates are required for securing these communications between the Persistent Agent and a FortiNAC Server (or a FortiNAC Control Server and FortiNAC Application Server pair). *See* Exhibit I, FortiNAC Deployment Guide at 32, "SSL Certificates" (excerpted) (available at https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e7ebbdaa-cabf-11ea-8b7d-00505692583a/FortiNAC_Deployment_Guide.pdf, last visited June 29, 2021); *see also*, Exhibit D, FortiNAC Administration Guide at 440.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "detecting the insecure condition includes" "receiving a response and determining whether the response includes

a valid digitally signed attestation of cleanliness." Fortinet denies the remaining allegations of paragraph 49.

50. FortiNAC agents are used to scan hosts and determine whether the host complies with the endpoint compliance policy assigned to that host. *See id.* at 438. Scans typically consist of lists of permitted operating systems and required antivirus software:

> Scans typically consist of lists of permitted operating systems and required antivirus software. In addition, custom scans can be created for more detailed scanning such as, searching the registry for particular entries, searching the hard drive for specific files, or verifying that hotfixes have been installed. Individual scans can be scheduled to run at regular intervals if your organization requires frequent rescans.
>
> The results of a scan are stored on the **Host Health** tab in the **Host Properties** view. Refer to Host health and scanning on page 722 for additional information.

See id. at 384 (underlining added). Each time a scan is run, a record of that scan is stored in the database and displayed on the Host Health tab of the Host Properties view:

> **Host health and scanning**
>
> Host health is determined by the endpoint compliance policies, system and administrative states, or scans run on the host. Each time a scan is run a record of that scan is stored in the database and displayed on the **Heath** tab of the **Host Properties** window. Each scan and scan type the host is eligible for is shown along with the name, status, and action. The agent scan shown in bold text and highlighted with a gray bar indicates the scan that is currently applied to the host. Click **Show History** for short-term historical data.

See id. at 722-23 (underlining added).

ANSWER: Fortinet denies the allegations of paragraph 50.

51. Therefore, the '705/'048 Accused Instrumentalities meet limitation B2 of claim 19.

ANSWER: Fortinet denies the allegations of paragraph 51.

52. Limitation C requires that "the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation C of claim 19. For example, endpoint compliance policies have many variables for the host scan. *See id.* at 423, "Scan parameters." For the antivirus and operating system variables, the scan can be narrowed by setting custom parameters. *See id.* The table below includes a subset of an alphabetical list of all the possible antivirus software parameters that can be configured for scanning Windows:

Parameter	Description	Typical options
AntiVirus definition Date	The date of the required AntiVirus definition files.	YYYY-MM-DD
AntiVirus Engine	The version number of the required AntiVirus Engine. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=

Parameter	Description	Typical options
Client Security Antimalware Service must be running	Select a setting.	Enabled or disabled
Client Security State Assessment Service must be running	Select a setting.	Enabled or disabled

See id. at 423. Therefore, the '705/'048 Accused Instrumentalities meet limitation C of claim 19.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." Fortinet denies the remaining allegations of paragraph 52.

53. Limitation D requires that "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation D of claim 19. For example, the "Quarantine VLAN Switching" option is enabled by default. *See id.* at 61. Under this option, if a host fails a scan, it is moved to the quarantine VLAN, which is separate from the production VLAN:

Option	Definition
Quarantine VLAN Switching	When quarantine VLAN Switching is set to Enable and the ports are in the Forced Remediation Group, the appliance switches unregistered hosts that are being scanned to the quarantine VLAN until the scan process is completed. Registered hosts are scanned in the production VLAN. Once the scan is finished and the registered host has passed, the host remains in the production VLAN. If the host fails the scan, it is moved to the quarantine VLAN to remediate. When set to Disable, all hosts remain in the production VLAN during the scan process even if the host fails the scan. Default =Enable

See id. at 61 (underlining added). Therefore, the '705/'048 Accused Instrumentalities meet limitation D of claim 19.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." Fortinet denies the remaining allegations of paragraph 53.

54. Limitation E1 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "receiving a service request sent by the first host [and] serving a quarantine notification page to the first host when the service request comprises a web server request." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation E1 of claim 19. For example, when a scan (including a custom scan) discovers that a host fails to meet a security policy, the browser is redirected to a web page with the results:

Results

Once the security check has completed, if the host failed to meet the security policy, a results page shown in a browser lists the items that failed and passed.

You can configure a link that the user can click that provides information about items that failed and what to do to correct the problem. Enter this link when you configure the policy. See Add or modify a scan on page 390 for more information.

If you do not provide a link, modify the failure page to provide information for the user to correct the problem and find assistance.

See id. at 459 (underlining added). Therefore, the '705/'048 Accused Instrumentalities meet limitation E1 of claim 19.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "preventing the first host from sending data to one or more other hosts associated with the protected network includes," "receiving a service request sent by the first host," "serving a quarantine notification page to the first host when the service request comprises a web server request." Fortinet denies the remaining allegations of paragraph 54.

55. Limitation E2 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation E2 of claim 19. For example, custom scans can result in redirecting the browser to a web page with details about the requirements that the host failed:

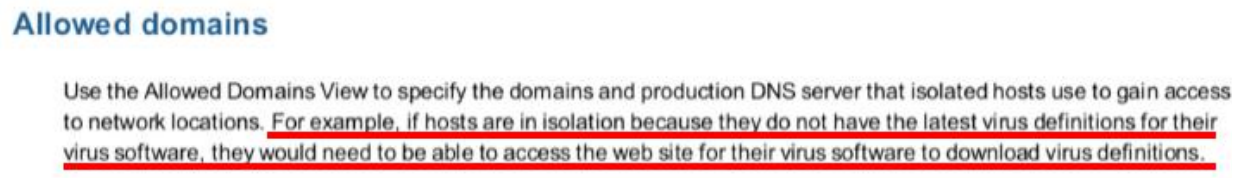
Required

When a custom scan severity level is set to **Required**, if the host fails the scan, the host is set to **At Risk**. The browser is redirected to a web page that contains details about the requirements the host failed. The host self-remediates (corrects the issues causing the failure) and rescans until it meets all requirements. When the host passes the requirements, it is moved to the production network.

See id. at 421 (underlining added). Therefore, the '705/'048 Accused Instrumentalities meet limitation E2 of claim 19.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "preventing the first host from sending data to one or more other hosts associated with the protected network includes," "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." Fortinet denies the remaining allegations of paragraph 55.

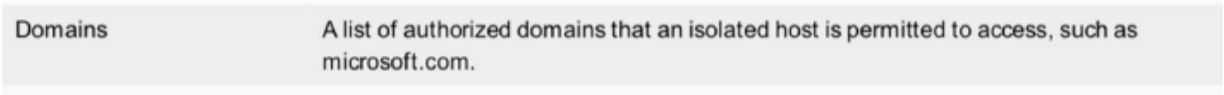
56. Limitation F requires "permitting the first host to communicate with the remediation host." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation F of claim 19. For example, FortiNAC can be configured with allowed domains that isolated hosts can access to remediate:



Allowed domains

Use the Allowed Domains View to specify the domains and production DNS server that isolated hosts use to gain access to network locations. For example, if hosts are in isolation because they do not have the latest virus definitions for their virus software, they would need to be able to access the web site for their virus software to download virus definitions.

See id. at 58 (underlining added).



Domains	A list of authorized domains that an isolated host is permitted to access, such as microsoft.com.

See id.

ANSWER: Fortinet admits that part of claim 19 of the '705 patent recites "permitting the first host to communicate with the remediation host." Fortinet denies the remaining allegations of paragraph 56.

57. Therefore, the '705/'048 Accused Instrumentalities meet limitation F of claim 19.

ANSWER: Fortinet denies the allegations of paragraph 57.

58. Accordingly, on information and belief, the '705/'048 Accused Instrumentalities meet all the limitations of, and therefore infringes, at least claim 19 of the '705 patent.

ANSWER: Fortinet denies the allegations of paragraph 58.

59. Fortinet indirectly infringes the claims of the '705 patent within the United States by inducing infringement under 35 U.S.C. § 271(b). For example, since learning of the '705 patent and by failing to cease offering the '705/'048 Accused Instrumentalities for sale, Fortinet has knowingly and intentionally induced users of the '705/'048 Accused Instrumentalities to directly infringe one or more claims of the '705 patent, inter alia, by (1) instructing users on how to use the '705/'048 Accused Instrumentalities in a manner that infringes the '705 Patent as described in the foregoing paragraphs; (2) providing customer support and training online and through its customer support call center on how to use them in an infringing manner; (3) directing its customers to additional online sources with instructions on how to infringe the '705 Patent (*see, e.g.*, https://training.fortinet.com/local/staticpage/view.php?page=library_fortinac; https://docs.fortinet.com/product/fortinac/9.1, last visited on September 15, 2021). Fortinet also posts information on publicly available websites such as channels on YouTube, which explain how to use the '705/'048 Accused Instrumentalities in an infringing manner (*see, e.g.*, https://www.youtube.com/c/Fortinet); and touting these infringing uses of the '705/'048 Accused Instrumentalities in advertisements, white papers, and product literature, including but not limited to those listed on or available from Fortinet's website.

ANSWER: Fortinet denies the allegations of paragraph 59.

60. Fortinet indirectly infringes the claims of the '705 patent by contributing to the direct infringement by end users under 35 U.S.C. § 271(c), for example, by providing the '705/'048 Accused Instrumentalities, which, as evidenced by Fortinet's websites and advertisements (*see, e.g.*, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf/, last visited on June 17, 2021), is especially made for use in a manner that infringes one or more claims of the '705 patent as described herein and have no substantial non-infringing uses.

ANSWER: Fortinet denies the allegations of paragraph 60.

61. As a result of Fortinet's infringement of the '705 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Fortinet's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Fortinet's wrongful conduct.

ANSWER: Fortinet denies the allegations of paragraph 61.

SECOND CAUSE OF ACTION
(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of '048 PATENT)

62. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

ANSWER: Fortinet repeats and re-alleges its responses to the preceding paragraphs of the First Amended Complaint as if those responses have been fully set forth herein.

63. On information and belief, Fortinet has directly and indirectly infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 17, of the '048 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to the '705/'048 Accused Instrumentalities.

ANSWER: Fortinet denies the allegations of paragraph 63.

64. For example, Claim 17 of the '048 patent recites the following:

> [preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes
>
> > [B1] contacting a trusted computing base associated with a trusted platform module within the first host,

> [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,
>
> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request
> >
> > [E2] wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page; and
>
> [F] permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition.

ANSWER: Fortinet admits that paragraph 64 appears to recite claim 17 of the '048 patent.

65. On information and belief, and based on publicly available information, at least the '705/'048 Accused Instrumentalities satisfy each and every limitation of at least claim 17 of the '048 patent.

ANSWER: Fortinet denies the allegations of paragraph 65.

66. The preamble recites a "computer program product for protecting a network." Regarding the preamble of claim 17, to the extent the preamble is determined to be limiting, the '705/'048 Accused Instrumentalities provide the features described in the preamble. *See, e.g.*, ¶¶ 39-41 ('705 patent preamble analysis). Thus, to the extent the preamble of claim 17 is limiting, the '705/'048 Accused Instrumentalities meet it.

ANSWER: Fortinet admits that part of the preamble of claim 17 of the '048 patent recites "computer program product for protecting a network." Fortinet denies the remaining allegations of paragraph 66.

67. Limitation A recites "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation A of claim 17. *See, e.g.*, ¶ 42 ('705 patent Limitation A analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation A of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." Fortinet denies the remaining allegations of paragraph 67.

68. Limitation B1 recites "wherein detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation B1 of claim 17. *See, e.g.*, ¶¶ 43-45 ('705 patent Limitation B1 analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation B1 of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "wherein detecting the insecure condition includes," "contacting a trusted computing base associated with a trusted platform module within the first host." Fortinet denies the remaining allegations of paragraph 68.

69. Limitation B2 recites "wherein detecting the insecure condition includes" "receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation B2 of claim 17. *See, e.g.*, ¶¶ 46-48 ('705 patent Limitation B2 analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation B2 of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "wherein detecting the insecure condition includes" "receiving a response, and determining whether the

response includes a valid digitally signed attestation of cleanliness." Fortinet denies the remaining allegations of paragraph 69.

70. Limitation C recites "wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation C of claim 17. *See, e.g.*, ¶ 49 ('705 patent Limitation C analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation C of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." Fortinet denies the remaining allegations of paragraph 70.

71. Limitation D recites "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation D of claim 17. *See, e.g.*, ¶ 50 ('705 patent Limitation D analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation D of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." Fortinet denies the remaining allegations of paragraph 71.

72. Limitation E1 recites "wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes" "receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a

web server request." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation E1 of claim 17. *See, e.g.*, ¶ 51 ('705 patent Limitation E1 analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation E1 of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes," "receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request." Fortinet denies the remaining allegations of paragraph 72.

73. Limitation E2 recites "wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation E2 of claim 17. *See, e.g.*, ¶ 52 ('705 patent Limitation E2 analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation E2 of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page." Fortinet denies the remaining allegations of paragraph 73.

74. Limitation F recites "permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition." The '705/'048 Accused Instrumentalities also meet all the requirements of limitation F of claim 17. *See, e.g.*, ¶¶ 53-54 ('705 patent Limitation F analysis). Thus, the '705/'048 Accused Instrumentalities meet limitation F of claim 17.

ANSWER: Fortinet admits that part of claim 17 of the '048 patent recites "permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition." Fortinet denies the remaining allegations of paragraph 74.

75. Accordingly, on information and belief, the '705/'048 Accused Instrumentalities meet all the limitations of, and therefore infringe, at least claim 17 of the '048 patent.

ANSWER: Fortinet denies the allegations of paragraph 75.

76. Fortinet indirectly infringes the claims of the '048 patent within the United States by inducing infringement under 35 U.S.C. § 271(b). For example, since learning of the '048 patent and by failing to cease offering the '705/'048 Accused Instrumentalities for sale, Fortinet has knowingly and intentionally induced users of the '705/'048 Accused Instrumentalities to directly infringe one or more claims of the '048 patent, inter alia, by (1) instructing users on how to use the '705/'048 Accused Instrumentalities in a manner that infringes the '048 Patent as described in the foregoing paragraphs; (2) providing customer support and training online and through its customer support call center on how to use them in an infringing manner; (3) directing its customers to additional online sources with instructions on how to infringe the '048 Patent (*see, e.g.*, https://training.fortinet.com/local/staticpage/view.php?page=library_fortinac; https://docs.fortinet.com/product/fortinac/9.1, last visited on September 15, 2021). Fortinet also posts information on publicly available websites such as channels on YouTube, which explain how to use the '705/'048 Accused Instrumentalities in an infringing manner (*see, e.g.*, https://www.youtube.com/c/Fortinet); and touting these infringing uses of the '705/'048 Accused Instrumentalities in advertisements, white papers, and product literature, including but not limited to those listed on or available from Fortinet's website.

ANSWER: Fortinet denies the allegations of paragraph 76.

77. Fortinet indirectly infringes the claims of the '048 patent by contributing to the direct infringement by end users under 35 U.S.C. § 271(c), for example, by providing the '705/'048 Accused Instrumentalities, which, as evidenced by Fortinet's websites and advertisements (*see, e.g.*, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf, last visited on June 17, 2021), is especially made for use in a manner that infringes one or more claims of the '048 patent as described herein and have no substantial non-infringing uses.

ANSWER: Fortinet denies the allegations of paragraph 77.

78. As a result of Fortinet's infringement of the '048 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Fortinet's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Fortinet's wrongful conduct.

ANSWER: Fortinet denies the allegations of paragraph 78.

THIRD CAUSE OF ACTION
(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of '892 PATENT)

79. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

ANSWER: Fortinet repeats and re-alleges its responses to the preceding paragraphs of the First Amended Complaint as if those responses have been fully set forth herein.

80. On information and belief, Fortinet has directly and indirectly infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 15 of the '892 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products, including but not limited to those, relating to the '892 Accused Instrumentalities.

ANSWER: Fortinet denies the allegations of paragraph 80.

81. On information and belief, Fortinet has been and currently is infringing the '892 patent by the manufacture, use, sale, offer to sell and/or importation of its products, including at least the '892 Accused Instrumentalities under 35 U.S.C. § 271.

ANSWER: Fortinet denies the allegations of paragraph 81.

82. For example, Claim 15 of the '892 patent recites the following:

> [preamble] A non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:
>
> [A] determining an identity relating to a person, wherein the identity is associated with the electronic document;
>
> [B] determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation;
>
> [C] determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation; and
>
> [D] determining a document reputation, wherein determining the document reputation uses the identity reputation.

ANSWER: Fortinet admits that paragraph 82 appears to recite claim 15 of the '892 patent.

83. On information and belief, and based on publicly available information, at least the '892 Accused Instrumentalities satisfy each and every limitation of at least claim 15 of the '892 patent.

ANSWER: Fortinet denies the allegations of paragraph 83.

84. The preamble of claim 15 recites a "non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address." Regarding the preamble of claim 15, to the extent the preamble is determined to be limiting, the '892 Accused Instrumentalities provide the features described in the preamble. For example, FortiMail "delivers advanced multi-layered protection against the full spectrum of email-borne threats." *See* Exhibit F, FortiMail Datasheet at 1.

ANSWER: Fortinet admits that part of the preamble of claim 15 of the '892 patent recites "non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address." Fortinet denies the remaining allegations of paragraph 84.

85. Further, FortiMail provides anti-spam functionality by using reputation analysis, that includes checks on IP, domain, and sender:

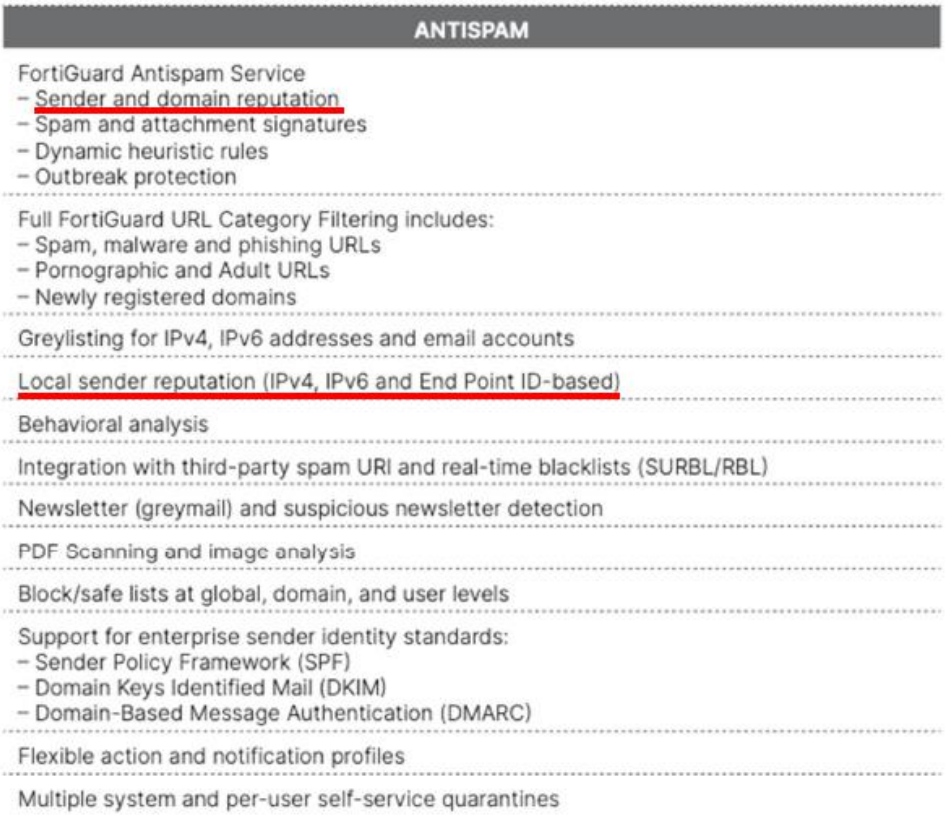
Multi-Layered Anti-Spam

Multiple sender, protocol and content inspection techniques shield users from spam and junk mail. Using a combination of reputation analysis, connection filtering, authentication and recipient verification methods allows for fast and accurate email protection. Checks include IP, domain, sender, SPF, DKIM, DMARC and geographical restrictions.

See id. at 2 (underlining added).

ANSWER: Fortinet denies the allegations of paragraph 85.

86. Specifically, FortiMail provides a local sender reputation feature, while the FortiGuard Antispam Service provides a sender and domain reputation feature:



ANTISPAM
FortiGuard Antispam Service – Sender and domain reputation – Spam and attachment signatures – Dynamic heuristic rules – Outbreak protection
Full FortiGuard URL Category Filtering includes: – Spam, malware and phishing URLs – Pornographic and Adult URLs – Newly registered domains
Greylisting for IPv4, IPv6 addresses and email accounts
Local sender reputation (IPv4, IPv6 and End Point ID-based)
Behavioral analysis
Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
Newsletter (greymail) and suspicious newsletter detection
PDF Scanning and image analysis
Block/safe lists at global, domain, and user levels
Support for enterprise sender identity standards: – Sender Policy Framework (SPF) – Domain Keys Identified Mail (DKIM) – Domain-Based Message Authentication (DMARC)
Flexible action and notification profiles
Multiple system and per-user self-service quarantines

See id. at 7 (underlining added).

ANSWER: Fortinet denies the allegations of paragraph 86.

87. Thus, to the extent the preamble of claim 15 is limiting, the '892 Accused Instrumentalities meet it.

ANSWER: Fortinet denies the allegations of paragraph 87.

88. Limitation A of claim 15 requires "determining an identity relating to a person, wherein the identity is associated with the electronic document." The '892 Accused Instrumentalities also meet all the requirements of limitation A of claim 15. For example, for each connecting SMTP client (sometimes called the sender), the Sender reputation feature records the sender IP address in the sender reputation database:

Check	Check Involves	Action If Positive	Action If Negative
Client initiates communication with the FortiMail unit			
Sender reputation	Client IP address	If the client IP is in the sender reputation database, check the score and enable any appropriate restrictions, if any.	Add the IP address to the sender reputation database and keep a reputation score based on the email received.

See Exhibit G, FortiMail Administration Guide at 26, 140 (underlining added).

ANSWER: Fortinet admits that part of claim 15 of the '892 patent recites "determining an identity relating to a person, wherein the identity is associated with the electronic document." Fortinet denies the remaining allegations of paragraph 88.

89. Therefore, the '892 Accused Instrumentalities meet limitation A of claim 15.

ANSWER: Fortinet denies the allegations of paragraph 89.

90. Limitation B of claim 15 requires "determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation." The '892 Accused Instrumentalities also meet all the requirements of limitation B of claim 15. For example, if the FortiGuard IP Reputation feature is enabled, FortiMail will query the FortiGuard Antispam service to determine if the SMTP client's public IP address is blocklisted. *See* Exhibit G, FortiMail Administration Guide at 420. FortiGuard further categorizes the blockedlisted IP addresses into three levels of reputation:

To configure FortiGuard scan options

1. When configuring an antispam profile, select the FortiGuard check box in the AntiSpam Profile dialog.
2. From Action, select the action profile that you want the FortiMail unit to use if the FortiGuard Antispam scan finds spam email. This action is the default action for all the FortiGuard filters, including IP reputation, URL filter, and spam outbreak protection.
   For more information, see Configuring antispam action profiles on page 429.
3. If you want the FortiMail unit to query the FortiGuard Antispam service to determine if the public IP address of the SMTP client is blocklisted, enable IP Reputation. If the SMTP client IP address is a private one, the FortiMail unit will query the FortiGuard Antispam service to determine if the first public IP address in the header is blocklisted.
   FortiGuard categorizes the blocklisted IP addresses into three levels – level 1 has the worst reputation, level 2 has better reputation, and level 3 has even better reputation. To help prevent false positives, you can choose to take different actions towards different IP reputation levels. Usually you should take strict actions, such as reject or discard, towards level 1 IP addresses while take loose actions, such as quarantine or tag, towards level 3 IP addresses. Using default actions for level 1, 2, and 3 means to use the IP Reputation action; using the default action for IP reputation means to use the FortiGuard action; and using the FortiGuard default action means to use the antispam profile action.
   If you want to check all SMTP servers in the `Received:` lines of the message header, enable the Extract IP from Received Header option.

See id. (underlining added).

ANSWER: Fortinet admits that part of claim 15 of the '892 patent recites "determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation." Fortinet denies the remaining allegations of paragraph 90.

91. Therefore, the '892 Accused Instrumentalities meet limitation B of claim 15.

ANSWER: Fortinet denies the allegations of paragraph 91.

92. Limitation C of claim 15 requires "determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation." The '892 Accused Instrumentalities also meet all the requirements of limitation C of claim 15. For example, FortiMail calculates a sender reputation score:

Viewing the sender reputation statuses

GUI item	Description
Search (button)	Click to filter the displayed entries. For more information, see Filtering sender reputation score entries on page 141.
IP	The IP address of the SMTP client.
Location	Lists the GeoIP locations/country names.
Score	The SMTP client's current sender reputation score.
State	Lists the action that the sender reputation feature is currently performing for delivery attempts from the SMTP client. • *Score controlled*: The action is determined by comparing the current *Score* value to the thresholds in the session profile.
Last Modified	Lists the time and date the sender reputation score was most recently modified.

Sender reputation is a predominantly automatic antispam feature, requiring little or no maintenance. For each connecting SMTP client (sometimes called a sender), the sender reputation feature records the sender IP address and the number of ***good*** email and ***bad*** email from the sender.

In this case, bad email is defined as:

- Spam
- Virus-infected
- Unknown recipients
- Invalid DKIM
- Failed SPF check

The sender reputation feature calculates the sender's current reputation score using the ratio of good email to bad email, and performs an action based on that score.

See Exhibit G, FortiMail Administration Guide at 140 (underlining added).

ANSWER: Fortinet admits that part of claim 15 of the '892 patent recites "determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation." Fortinet denies the remaining allegations of paragraph 92.

93. Therefore, the '892 Accused Instrumentalities meet limitation C of claim 15.

ANSWER: Fortinet denies the allegations of paragraph 93.

94. Limitation D of claim 15 requires "determining a document reputation, wherein determining the document reputation uses the identity reputation." The '892 Accused Instrumentalities also meet all the requirements of limitation D of claim 15. For example, to determine which action the FortiMail unit will perform after it calculates the sender reputation score, the FortiMail unit compares the sender reputation score to three configurable score thresholds:

To determine which action the FortiMail unit will perform after it calculates the sender reputation score, the FortiMail unit compares the score to three score thresholds which you can configure in the session profile:

1. **Throttle client at:** For scores less than this threshold, senders are allowed to deliver email without restrictions. For scores greater than this threshold but less than the temporary fail threshold, senders are rate-limited in the number of email messages that they can deliver per hour, expressed as either an absolute number or as a percentage of the number sent during the previous hour. If a sender exceeds the limit and keeps sending email, the FortiMail unit will send temporary failure codes to the sender. See descriptions for *Temporary fail* in Configuring sender reputation options on page 399.
2. **Temporarily fail:** For scores greater than this threshold but less than the reject threshold, the FortiMail unit replies to senders with a temporary failure code, delaying delivery and requiring senders to retry later when their score is reduced.
3. **Reject:** For scores greater than this threshold, the FortiMail unit replies to senders with a rejection code.

See Exhibit G, FortiMail Administration Guide at 140-141.

ANSWER: Fortinet admits that part of claim 15 of the '892 patent recites "determining a document reputation, wherein determining the document reputation uses the identity reputation." Fortinet denies the remaining allegations of paragraph 94.

95. Therefore, the '892 Accused Instrumentalities meet limitation D of claim 15.

ANSWER: Fortinet denies the allegations of paragraph 95.

96. Accordingly, on information and belief, the '892 Accused Instrumentalities meet all the limitations of, and therefore infringe, at least claim 15 of the '892 patent.

ANSWER: Fortinet denies the allegations of paragraph 96.

97. Fortinet indirectly infringes the claims of the '892 patent within the United States by inducing infringement under 35 U.S.C. § 271(b). For example, since learning of the '892 patent and by failing to cease offering the '892 Accused Instrumentalities for sale, Fortinet has knowingly and intentionally induced users of the '892 Accused Instrumentalities to directly infringe one or more claims of the '892 patent, inter alia, by (1) instructing users on how to use the '892 Accused Instrumentalities in a manner that infringes the '892 Patent as described in the foregoing paragraphs; (2) providing customer support and training online and through its customer support call center on how to use them in an infringing manner; (3) directing its customers to additional online sources with instructions on how to infringe the '892 Patent (*see, e.g.*, https://www.fortinet.com/products/email-security, last visited on September 15, 2021). Fortinet also posts information on publicly available websites such as channels on YouTube, which explain how to use the '892 Accused Instrumentalities in an infringing manner (*see, e.g.*, https://www.youtube.com/c/Fortinet); and touting these infringing uses of the '892 Accused Instrumentalities in advertisements, white papers, and product literature, including but not limited to those listed on or available from Fortinet's website.

ANSWER: Fortinet denies the allegations of paragraph 97.

98. Fortinet indirectly infringes the claims of the '892 patent by contributing to the direct infringement by end users under 35 U.S.C. § 271(c), for example, by providing the '892 Accused Instrumentalities, which, as evidenced by Fortinet's websites and advertisements (*see, e.g.*, https://www.fortinet.com/products/email-security, last visited on September 15, 2021), is especially made for use in a manner that infringes one or more claims of the '892 patent as described herein and have no substantial non-infringing uses.

ANSWER: Fortinet denies the allegations of paragraph 98.

99. As a result of Fortinet's infringement of the '892 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Fortinet's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Fortinet's wrongful conduct.

ANSWER: Fortinet denies the allegations of paragraph 99.

AFFIRMATIVE AND OTHER DEFENSES

1. Without altering the burdens of proof, Fortinet asserts the following affirmative and other defenses. Fortinet reserves the right to amend its answer with additional defenses as further information is obtained.

FIRST AFFIRMATIVE DEFENSE: NON-INFRINGEMENT

2. Fortinet alleges that it does not infringe and has not infringed, directly, indirectly or jointly, literally or by the doctrine of equivalents, any valid and enforceable claim of the ’705 patent.

3. Fortinet alleges that it does not infringe and has not infringed, directly, indirectly or jointly, literally or by the doctrine of equivalents, any valid and enforceable claim of the ’048 patent.

4. Fortinet alleges that it does not infringe and has not infringed, directly, indirectly or jointly, literally or by the doctrine of equivalents, any valid and enforceable claim of the ’892 patent.

SECOND AFFIRMATIVE DEFENSE: INVALIDITY

5. The claims of ’705 patent are invalid, unenforceable and/or void for failure to satisfy one or more of the requirements for patentability set forth in Title 35 of the United States Code, including without limitation 35 U.S.C. §§ 101, 102, 103, 112, and/or 282.

6. The claims of ’048 patent are invalid, unenforceable and/or void for failure to satisfy one or more of the requirements for patentability set forth in Title 35 of the United States Code, including without limitation 35 U.S.C. §§ 101, 102, 103, 112, and/or 282.

7. The claims of ’892 patent are invalid, unenforceable and/or void for failure to satisfy one or more of the requirements for patentability set forth in Title 35 of the United States Code, including without limitation 35 U.S.C. §§ 101, 102, 103, 112, and/or 282.

THIRD AFFIRMATIVE DEFENSE: LIMITATIONS ON DAMAGES AND RECOVERY

8. Pursuant to the requirements of 35 U.S.C. §§ 286-288, the Plaintiff's ability to recover damages and/or costs is limited.

9. As a matter of law, plaintiff is not entitled to any purported damages suffered more than six (6) years prior to the filing of the Complaint.

10. On information and belief, plaintiff failed to mark its products or services incorporating the purported invention(s) of the patents-in-suit with the number of the applicable patent as required by 35 U.S.C. § 287. Plaintiff also failed to require its licensees to mark products and services offered under a license of any or all of the patents-in-suit.

11. Plaintiff failed to provide actual notice of the patents-in-suit to Fortinet prior to the filing of the Original Complaint.

12. Fortinet did not have actual notice of the patents-in-suit under 35 U.S.C. § 287 prior to the filing of the Original Complaint.

13. Plaintiff is not entitled to damages constituting a reasonable royalty prior to the filing of the Original Complaint because Plaintiff's failed to mark its products and services or provide Fortinet actual notice of the patents-in-suit as required by 35 U.S.C. § 287.

14. Plaintiff is barred by 35 U.S.C. § 288 from recovering costs associated with this action.

15. Plaintiff is not entitled to treble damages under 35 U.S.C. § 284 because Plaintiff has failed to meet, and cannot meet as a matter of law, the requirements for willful infringement.

16. The extent certain products accused of infringing the Asserted Patents are used by and/or manufactured for the United States Government, Plaintiff's claims against Fortinet with respect to such products may not be pursued in this Court and are subject to other limitations pursuant to 28 U.S.C. § 1498.

FOURTH AFFIRMATIVE DEFENSE: PROSECUTION HISTORY ESTOPPEL

17. Plaintiff's claims of patent infringement are barred in whole or in part by the doctrine of prosecution history estoppel. K.Mizra is estopped, based on the amendments, arguments, statements, representations, admissions, or omissions during the prosecution of the patents applications or any related provisional or non-provisional applications, made with respect to the scope of the invention and asserted claims and disclosure of the prior art, and upon which the examiners at the United States Patent and Trademark Office relied in the allowance of the claims of the '705 patent, the '048 patent, and the '892 patent, from asserted any interpretation of any of the patent claims that would be broad enough to cover any of the alleged infringement by Fortinet.

FIFTH AFFIRMATIVE DEFENSE: LACHES AND WAIVER

18. Plaintiff's claims are barred, in whole or in part, by the doctrine of laches and/or waiver.

SIXTH AFFIRMATIVE DEFENSE: LICENSE

19. Plaintiff's claims are barred by license or implied license.

SEVENTH AFFIRMATIVE DEFENSE: ESTOPPEL

20. Plaintiff's claims are barred by estoppel.

EIGHTH AFFIRMATIVE DEFENSE: INJUNCTIVE RELIEF UNAVAILABLE

21. K.Mizra is not entitled to injunctive relief because any alleged injury to K.Mirza is neither immediate nor irreparable, and K.Mizra has an adequate remedy at law.

Fortinet reserve the right to amend their Answer to add additional Affirmative Defenses under Rule 8(c) of the Federal Rules of Civil Procedure, the Patent Laws of the United States, and any other defenses, at law and equity (including but not limited to instances of inequitable conduct, unclean hands, patent misuse, and/or implied license) as they become known throughout the course

of discovery in this case. Assertion of a defense is not a concession that Fortinet has the burden of proving the matter asserted.

COUNTERCLAIMS FOR DECLARATORY JUDGMENT

Counterclaim-Plaintiff Fortinet, on personal knowledge as to its own acts, and on information and belief as to all others based on its own and its attorneys' investigation, alleges Counterclaims against Fortinet as follows:

NATURE OF THE ACTION

1. These Counterclaims arise from K.Mizra's baseless allegations of infringement against Fortinet.

2. According to the allegations set forth in the First Amended Complaint, K.Mizra claims to be the owner of all rights, titles, and interests to the '705 patent, the '048 patent, and the '892 patent, including the rights to sue and recover for infringement.

3. K.Mizra has accused Fortinet of directly infringing, contributing to the infringement of, or inducing others to infringe the 'the '705 patent, the '048 patent, and the '892 patent. Fortinet denies that any of its products infringe any valid or enforceable claim of the '705 patent, the '048 patent, and the '892 patent.

4. An actual case and controversy exists between the parties concerning the infringement of one or more claims of the '705 patent, the '048 patent, and the '892 patent, and that controversy is ripe for adjudication by this Court.

JURISDICTION AND VENUE

5. These are Counterclaims for a declaration of non-infringement and invalidity of one or more claims of the '705 patent, the '048 patent, and the '892 patent. This Court has subject matter jurisdiction over these Counterclaims pursuant to 28 U.S.C. §§ 1331, 1338, and 2201. This

Court also has personal jurisdiction over K.Mizra because K.Mizra has already submitted to the jurisdiction of this judicial district by initiating the instant lawsuit.

6. Venue for these Counterclaims is legally proper in this District pursuant to 28 U.S.C. §§ 1367 and 1391, although venue is more appropriate and convenient in another District.

PARTIES

7. Counterclaim-Plaintiff Fortinet is a Delaware corporation with a principal place of business at 899 Kifer Road Sunnyvale, CA 94086 USA.

8. According to the allegations in paragraph 5 of the First Amended Complaint, K.Mizra LLC ("K.Mizra") is a Delaware limited liability company with its principal place of business at 777 Brickell Ave, #500-96031, Miami, FL 33131.

COUNTERCLAIM COUNT I
(Non-Infringement of U.S. Patent No. 8,234,705)

9. Fortinet repeats and re-alleges the allegations contained in paragraphs 1 through 8 as if fully set forth herein.

10. Fortinet is neither infringing, contributorily infringing, actively inducing others to infringe, nor otherwise liable under 35 U.S.C. § 271 for infringement of any claim of the '705 patent as properly construed.

11. To resolve the legal and factual questions raised by K.Mizra and to afford relief from the uncertainty and controversy that K.Mizra's accusations have precipitated, Fortinet is entitled to declaratory judgment that it has not infringed and is not infringing, directly or indirectly, any valid, enforceable claim of the '705 patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM COUNT II
(Invalidity of U.S. Patent No. 8,234,705)

12. Fortinet repeats and re-alleges the allegations contained in paragraphs 1 through 8 as if fully set forth herein.

13. One or more claims of the '705 patent are invalid or unenforceable for failing to meet one or more of the requisite statutory and decisional requirements and/or conditions for patentability under one or more of 35 U.S.C. §§ 41, 101, 102, 103, 112, and 116.

14. To resolve the legal and factual questions raised by K.Mizra and to afford relief from the uncertainty and controversy from which K.Mizra's accusations have precipitated, Fortinet is entitled to a declaratory judgment that the '705 patent is invalid.

COUNTERCLAIM COUNT III
(Non-Infringement of U.S. Patent No. 9,516,048)

15. Fortinet repeats and re-alleges the allegations contained in paragraphs 1 through 8 as if fully set forth herein.

16. Fortinet is neither infringing, contributorily infringing, actively inducing others to infringe, nor otherwise liable under 35 U.S.C. § 271 for infringement of any claim of the '048 patent as properly construed.

17. To resolve the legal and factual questions raised by K.Mizra and to afford relief from the uncertainty and controversy that K.Mizra's accusations have precipitated, Fortinet is entitled to declaratory judgment that it has not infringed and is not infringing, directly or indirectly, any valid, enforceable claim of the '048 patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM COUNT IV
(Invalidity of U.S. Patent No. 9,516,048)

18. Fortinet repeats and re-alleges the allegations contained in paragraphs 1 through 8 as if fully set forth herein.

19. One or more claims of the '048 patent are invalid or unenforceable for failing to meet one or more of the requisite statutory and decisional requirements and/or conditions for patentability under one or more of 35 U.S.C. §§ 41, 101, 102, 103, 112, and 116.

20. To resolve the legal and factual questions raised by K.Mizra and to afford relief from the uncertainty and controversy from which K.Mizra's accusations have precipitated, Fortinet is entitled to a declaratory judgment that the '048 patent is invalid.

COUNTERCLAIM COUNT V
(Non-Infringement of U.S. Patent No. 8,965,892)

21. Fortinet repeats and re-alleges the allegations contained in paragraphs 1 through 8 as if fully set forth herein.

22. Fortinet is neither infringing, contributorily infringing, actively inducing others to infringe, nor otherwise liable under 35 U.S.C. § 271 for infringement of any claim of the '892 patent as properly construed.

23. To resolve the legal and factual questions raised by K.Mizra and to afford relief from the uncertainty and controversy that K.Mizra's accusations have precipitated, Fortinet is entitled to declaratory judgment that it has not infringed and is not infringing, directly or indirectly, any valid, enforceable claim of the '892 patent, either literally or under the doctrine of equivalents.

COUNTERCLAIM COUNT VI
(Invalidity of U.S. Patent No. 8,965,892)

24. Fortinet repeats and re-alleges the allegations contained in paragraphs 1 through 8 as if fully set forth herein.

25. One or more claims of the '892 patent are invalid or unenforceable for failing to meet one or more of the requisite statutory and decisional requirements and/or conditions for patentability under one or more of 35 U.S.C. §§ 41, 101, 102, 103, 112, and 116.

26. To resolve the legal and factual questions raised by K.Mizra and to afford relief from the uncertainty and controversy from which K.Mizra's accusations have precipitated, Fortinet is entitled to a declaratory judgment that the '892 patent is invalid.

DEMAND FOR JURY TRIAL

27. Fortinet requests a trial by jury of all issues in this action triable by jury.

PRAYER FOR RELIEF

WHEREFORE, Fortinet prays that this Court enter a judgment in its favor and against K.Mizra as follows:

A. Entry of judgment in favor of Fortinet and against K.Mizra thereby fully and finally dismissing K.Mizra's First Amended Complaint in its entirety, with prejudice, with K.Mizra taking nothing by way of its claims;

B. Entry of judgment that K.Mizra is not entitled to any of its requested relief, or any relief whatsoever;

C. Entry of judgment that Fortinet be awarded its costs and disbursements in this action;

D. Entry of judgment that this case be declared exceptional pursuant to 35 U.S.C. § 285 and that Fortinet be awarded its reasonable attorneys' fees and costs in this action; and

E. Entry of judgment granting Fortinet such other relief as the Court deems just and proper.

DATED: October 18, 2021

Respectfully submitted,

By: */s/ J. Mark Mann*

J. Mark Mann
State Bar No. 12926150
mark@themannfirm.com
G. Blake Thompson
State Bar No. 24042033
blake@themannfirm.com
Mann | Tindel | Thompson
201 East Howard
Henderson, TX 75654
Telephone: 903-657-8540
Facsimile: 903-657-6003

Andrew M. Holmes (admitted in E.D. Tex.)
California Bar #260475
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, CA 94111
415-875-6600
415-875-6700 (Facsimile)
drewholmes@quinnemanuel.com

Attorneys for Fortinet, Inc.

CERTIFICATE OF SERVICE

I hereby certify that counsel of record who are deemed to have consented to electronic service are being served today, October 18, 2021, with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a).

/s/ *J. Mark Mann*
J. Mark Mann